The Importance of Information Security for Financial Institutions and Proposed Countermeasures

— With a Focus on Internet-Based Financial Services —

(Overview)

1. In recent years, the development of information technology (IT) has brought with it a rapid increase in the use of open network systems, as typified by the Internet, to provide financial services. Concurrently, proper management of information security risks such as the risk of service interruptions, theft or alteration of data, impersonation and other events resulting from unauthorized access to the computer system is rapidly becoming critical.

2. If these risks should occur and cause unauthorized remittances and service interruptions, not only could the business of individual financial institutions be adversely affected, but the entire settlement system could also be impacted. In order to ensure sound development of the financial services sector, while reaping the benefits from the remarkable advance of the IT revolution, it is vital for each financial institution to become thoroughly cognizant of the importance of information security, and to work for managing risk systematically throughout the organization in line with each situation, under the active involvement of management.

3. In this recognition, we have put together a list of points in this paper about the importance of information security and measures thereof in an effort to assist financial institutions in implementing appropriate information security countermeasures and safeguards.

April 18, 2000

Bank of Japan

Table of Contents

For more details regarding information security issues, please visit the Web site of Bank of Japan's Institute for Monetary and Economic Studies <http://www.imes.boj.or.jp/english/>, which contains a number of works on technical subjects such as encryption and authentication, and Bank of Japan's Web site <http://www.boj.or.jp/en/> for related works.

1. Introduction

With the rapid advances in information technology (IT)[1], which have taken place in recent years, institutions in the financial services sector have actively begun to utilize systems using open network as typified by the Internet (hereafter referred to as open systems[2]).

In the system formerly adopted by most financial institutions, the users authorized to make access to the network have been limited (hereafter referred to as closed systems). Therefore in implementing security measures, emphasis was placed on the prevention of unauthorized acts by financial institution employees that engage in the system.

Meanwhile, although the use of open systems has opened the way to provide more convenient financial services, it has also diversified and complicated the nature of risks. In other words, while risks such as system breakdowns and unauthorized acts by employees have existed regardless of closed or open system environment, with the increased reliance on open systems, there are now greatly increased risks such as third parties' impersonating clients and theft or alteration of information transmitted over networks. Furthermore, there is the emergence of new risks, such as unauthorized access from the outside and service interruptions that are specific to open systems (In this paper, risks that accompany the use of open systems are represented by the term "information security risk"[3]).

In order to adequately manage these information security risks that are becoming ever

[1] IT (information technology) is defined as the full range of information and communication technology, related to computers and network infrastructure.
[2] Open systems are generally defined by the characteristics of the network comprising the system. In some cases however, they refer to such systems whose software models are open to public, or systems in which processing is distributed among multiple computers and overall processing is done through mutual linkages (as UNIX).
[3] Generally speaking, information security usually means "to rightly protect an organization's proprietary information and information systems (Confidentiality), maintain its authenticity (Integrity), and assure its effective use when necessary(Availability)".

more diversified and complex, financial institutions are urged first of all to ascertain the nature of risk, and then to establish the required security measures and work toward their unswerving implementation, in the same way as they manage other risks.[4]

This paper points out the core aspects of information security risk management by financial institutions. The paper utilizes the expertise Bank of Japan has accumulated through surveys, research, examination, and consultation with relevant domestic and foreign institutions, as well as the experience gained through the systems that the Bank operates itself.[5] The attached "Checklist of Information Security Measures for Systems That Make Use of the Internet" points out major items for checking the information security measures in individual systems that use the Internet. It is expected that the attachment, together with this paper, serves financial institutions in developing and implementing their information security measures.

2. The Heightening of Information Security Risks

(1) The Move toward Open Systems and Information Security Risks

Japanese financial institutions are becoming aware that, with the rapid changes in the business environment, it is critical for management to provide customers with convenient financial services quickly and inexpensively. To achieve this goal, financial institutions have been progressively utilizing IT, which has undergone amazing advances in recent years.[6]

---

[4] Throughout Japan, there has recently been a dramatic increase in awareness of the importance of dealing with information security issues. A law prohibiting unauthorized access took effect in February 2000, a bill concerning digital signatures and authentication is being developed, and other efforts have been made with the aim of realizing a "Digital Government."

[5] Financial institutions have already implemented comparatively stringent measures in connection with information security measures for closed systems, so this paper will not deal with such measures (for details, please refer to publications on standards for computer system security released by the Center for Financial Industry Information Systems [FISC] and other documents).

[6] The financial industry is a classic example of information industries, in the sense that its products are intangible and data processing serves as the core of its business, so the question of how to maximize the leverage gained from IT has become a key issue in the management of financial institutions. In fact, one of the goals in the recent trend of the integration of financial institutions has been to make large-scale IT investments more efficient.

There has been a particularly large amount of technical innovation in the area of open systems typified by the Internet, and that has made it possible to build such open systems much more cheaply and quickly than conventional systems and to provide service to a broader range of customers as well. The financial industry is also aware that a speedy response to the managerial issues of establishing a customer base is critical, and consequently more financial institutions use the Internet as a way to achieve this.[7]

Meanwhile, this increased reliance on IT and the expanded use of open system in the financial services sector propagates information security risk that requires new countermeasures for risk management by individual financial institutions.

(The Occurrence of New Risks and Increase in Existing Risks)

Japanese financial institutions have implemented security measures that are predicated on the use of closed systems based primarily on mainframe computers, such as (a) physical separation through management of entrances and exits of computer centers and through the construction of networks with leased lines, (b) the use of customized software and communication protocols (rules), and (c) monitoring using security cameras and human surveillance in branch. Due to the use of such measures, security invasions from the outside have been relatively rare in these closed systems.

Nevertheless, with the increasing move toward open systems, it is much easier now to gain unauthorized access from the outside and theft of data than in the past. The internal business processing systems of financial institutions are being connected with other outside networks, and we see a greater use of common communication protocol. Moreover, there are many devices used for customer transactions that may be managed

[7] In addition to the noticeable trend of existing financial institution to launch Internet banking services, there has also been activity in the establishment of banks specialized in Internet banking and securities companies specialized in online trading, including business by companies from outside the financial

by financial institutions less sufficiently than cash dispensers and automatic teller machines (ATMs).

As a result, (a) the risk of unauthorized access to internal systems (hacking) and of service interruptions has arisen. Moreover, existing risks such as (b) illegal acquisition of personal identification numbers (PINs) by theft of data in the network, (c) unauthorized remittances through alteration of data, and (d) the acquisition of funds through impersonation of parties to a transaction, has increased significantly (See Diagram 1).

For example, as for unauthorized access and service interruptions, even organizations that have implemented advanced security measures, including governmental organizations in the United States, have experienced damage from hackers from time to time. In Japan, since January 2000, information published on the Web sites of government ministries and agencies was altered and service had to be suspended. The number of financial institutions that experience information security infringements is increasing. In addition, there are examples of service interruptions occurring as a result of service-provider systems being halted through orchestrated accesses aimed at overloading system capacities.[8] If this situation were to occur with financial services involving the transfer of funds or other transactions, massive impact[9] that dwarfs the mere suspension of information services would inevitably reverberate not only within such financial institutions but also throughout the entire settlement system.

---

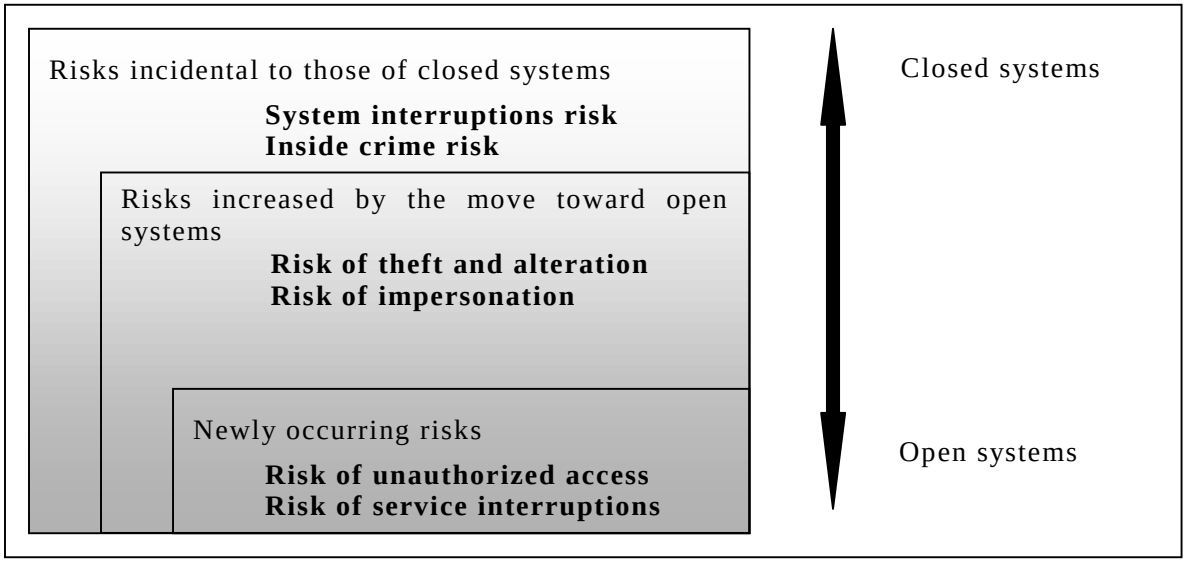
industry.

[8] In February 2000, an overseas securities company specializing in online trading was forced to suspend services by orchestrated accesses aimed at overloading system capacities.

[9] A major U.S. bank has already suffered from unauthorized access for dozens of times, resulting in an unauthorized fund transfer of more than US $10 million.

Diagram 1

Increased Usage of Open Systems and the Occurrence of New Risks



(Points of Concern due to Increased Outsourcing)

In recent years, financial institutions have employed a variety of means of outsourcing such as entrusting their subsidiaries or specialized firms with works ranging from system development to system operation. As a result, there are more financial institutions that do not directly manage their systems subject to information security. In this case, there is a risk of information leaks. In response, precautionary measures are necessary to ensure that institutions remain focused on their own security through clarifying strict provisions in outsourcing contracts and maintaining system audit rights and similar safeguards.

(2) Impact on Financial Services

If information security risks such as service interruptions and unauthorized access should occur at an individual financial institution, the financial institution may have to suspend services temporarily. In this case, in addition to service interruptions, the financial institution might also suffer significantly from management aspects. For example, the institution might run a reputational (rumor) risk if its credibility is compromised, and the legal risk of a lawsuit on account of lacking adequate information

security safeguards.

In recent years, various settlements between financial institutions have been systemized to a large degree. Therefore, if a breakdown should occur and the system cease to operate at a given financial institution, not only may the given financial institution have difficulty in continuing its business, but this adverse influence may very quickly spread through the entire settlement system. Financial institutions must very seriously consider the risk that a system breakdown could go beyond being their own problem to having a significant adverse impact on other participants in the settlement system. Thus, these financial institutions need to both refine measures to prevent this from happening ahead of time as well as to prepare contingency plans for a quick recovery.[10]

3. Formulating Information Security Policies

Because of the greater usage of open systems for a financial institution's many business processing needs, a variety of business units within those organizations are under pressure to implement information security measures. For the entire organization to work together and effectively implement countermeasures under these conditions, policies and their specific details should be written, and then it must be ensured that the entire organization is notified thoroughly.

Although Japanese financial institutions do have experience at employing measures for information security, in many instances these measures seem to have been devised on an individual system basis, and Japanese financial institutions are behind their counterparts in Europe and North America when it comes to cross-sectional countermeasures covering the entire system. Nevertheless, as the use of open systems increases, there is a cogent need to grasp the information security risks facing the entire

[10] For more on the need for individual financial institutions to manage settlement risk, including the risk of system breakdowns, refer to "Settlement Risk Management of Financial Institutions" (published in February 2000, available only in Japanese).

organization accurately and to establish policies and standards that are necessary for the formulation and implementation of appropriate countermeasures.

(1) What Is Information Security Policy?

Information security policy[11] is the systemization of approaches and policies related to the formulation of information security measures to be applied within an organization in order to respond to the needs as outlined above. It is a policy on safeguards aimed at taking proper precautions to ensure security of information and information systems owned by an organization. Generally speaking, in most cases it consists of a "basic approach to information security measures (basic policy)" and "measures and standards applicable throughout the organization (standards)".[12] Table 1 lists items that are normally included in basic information security policy.

Table 1

Examples of Items in Basic Information Security Policy

(1) Purpose and scope of information security measures • Basic approach to information security measures • The information and information systems that must be protected, and the reasons for such protection • Priorities of information and information systems that must be protected
(2) Mechanisms to promote information security measures

[11] The Financial Supervisory Agency indicated the importance of information security policy as a part of risk management in the Financial Inspection Manuals published in 1999. Additionally a guide to formulating security policies for financial institutions released by FISC in 1999 contains a detailed explanation of procedures to formulate policies and similar information.

[12] Additionally, in some cases this also includes documents noting specific information security measures in each individual sector (rules, manuals, procedures, and similar information). As for the procedures for formulating information security policy, it is important first of all to specify the information and information systems requiring protection, and by taking note of the importance and potential threat of those systems, to formulate the "basic policy." It is desirable next to set standards that each information security measure should satisfy, based on a risk assessment by considering the probability of the occurrence of hypothesized risks as well as loss if such risks were to occur.

- Involvement and responsibility of management, appointment of an executive responsible for information security, and establishment of an information security coordination division
- Checks by the legal department and compliance with laws and regulations
- The use of outside consultants or similar business advisors

(3) The implementation of information security measures
- Presumable information security risks and their management
- Decision-making process of implementing information security measures
- Procedures for revising information security measures
- Overview of the contents of information security measures

(4) Management of users and training for information security
- Responsibilities of each executive and employees and rules to be applied in case of violations (penalties, etc.)
- Checking the status of compliance with formulated information security measures by self-checking and internal inspection
- Enlightenment on information security policy

(5) Crisis management
- Responding to breakdowns in computer systems

(6) Other
- Procedures for periodically reevaluating information security policies

(2) Efficacy of Information Security Policy

The formulation of information security policy is expected to bring financial institutions the efficacy of enhanced security levels as shown in Table 2 made possible by the implementation of comprehensive and effective information security measures for the entire organization.

Table 2

Efficacy of Information Security Policy

(1) An increased awareness of the importance of information security within organizations is expected particularly within management, then the necessary resources are devoted to information security measures.

- The understanding of information security policy throughout the entire organization will facilitate necessary investment of resources. In addition in the process of developing individual systems, this will also provide incentives for implementation of necessary security measures.

(2) By formulating security measures in accordance with consistent standards, a given level of information security is assured within the whole organization.

(3) The weak points of previously implemented information security measures will become clear, and the understanding of risks will be facilitated.

- For example, the formulation of the information security policy will provide the opportunity for reviewing the traditional information security measures, such as a further shift toward using Integrated Circuit cards (IC cards),[13] which is promoted by financial institutions.[14] If these institutions continue to use magnetic stripe cards in open systems, it will require them to implement additional measures to improve security levels.

(4) When new systems are developed, it will be possible to review information security measures of these systems efficiently.

(5) If a problem with information security should occur, a quick response can be expected.

[13] The debit card that has been extended on a large scale since March 2000, in Japan utilizes magnetic stripe cards and has some aspects of open system, such as the partial use of public lines. Therefore, in comparison to the cash dispensers and ATMs that use the same card, stronger risk management measures such as the conversion to IC cards needs to be considered.

[14] For example, scrambling technique (easy method of transforming data by applying arithmetical operations and the processing method is kept secret)is considered insufficient to achieve confidentiality of data. It is desirable to consider, while referencing international standards and similar norms, the use of authentic encryption technology.

(3) Establishing Information Security Policy as a Management Issue

(The Importance of an Organizational Response with the Strong Involvement of the Management)

As already explained, both the importance of IT and risks inherent to IT are increasing for financial institutions. Therefore, it becomes clear that the management of information security risk on an organization-wide basis is one of the critical issues for management.

In order to ensure the required security level, it is necessary to dedicate the appropriate management resources and to gain adequate understanding and cooperation from each business unit within the financial institutions. However, it is difficult for executives and staff to normally sense the direct advantages of information security measures, and consequently, it is not easy to promote these measures in a bottom-up fashion. Thus, taking into account their own IT strategies, management is recommended to take an active role in the risk management process. This may be done, for example, by ensuring that management receives an accurate picture of information security risks and propose the necessary measures.

(Notification and Implementation of Information Security Policy)

Specifically, there is a need to create a clear and strong sense that the entire organization must adhere to this policy by formulating information security policy under the leadership of management. The responsibilities of each business unit related to information security and rules, lest problems arise due to breaches of policy, should be clear to all within the organization.[15]

If cases that violate information security policy are discovered when periodically assessing information security risks, it is crucial that required measures be proposed by

[15] It is preferable that a person responsible for managing information security be appointed and that financial institutions establish an information security controlling unit, which is independent of user departments and the systems development department, in accordance with the size and operation of the

the responsible business unit, and that procedures be established to allow the unit or person responsible for controlling the entire organization to approve these measures for each case. Additionally, it is beneficial to the improvement of effectiveness of information security policy that the condition of compliance with the policy be verified by internal audits or inspections.

The periodic revision of information security policies is necessary. If there is even only one hole in information security, there is a risk that unauthorized access or other harmful acts may occur. Thus, it is important to periodically confirm the latest information on security and to establish mechanisms in a daily course of business for checking the security policy itself as necessary.

(Compatibility with International Standards)

As global business operations and connection of systems develop, Japanese financial institutions will be required to ensure that their information security policies are compatible with international standards. To achieve this, it is preferable that they evaluate the suitability of their own measures regularly, while giving consideration to the latest technology trends and properly referring to international standards and guidelines[16] formulated by the ISO (International Organization for Standardization).

---

financial institution.

[16] In addition to the previously mentioned FISC guide, the below-listed guidelines provide reference on international standards for information security. For details, please refer to the following two documents both by the Institute for Monetary and Economic Studies, Bank of Japan: "Trends Toward International Standardization of Information Security Technology for the Financial Sector"(*Kinyu-Kenkyu* Vol. 18, No. 2, 1999, available only in Japanese) and "Recent Trends Concerning Evaluation and Certification of Information Security for Financial Services"(IMES Discussion Paper Series 99-J-44, available only in Japanese).

(1) BS(British Standards)7799: Code of practice for information security management
(2) ISO/TR13569: Banking and related financial services - Information security guidelines
(3) ISO15408: Information technology - Security techniques - Evaluation criteria for IT security

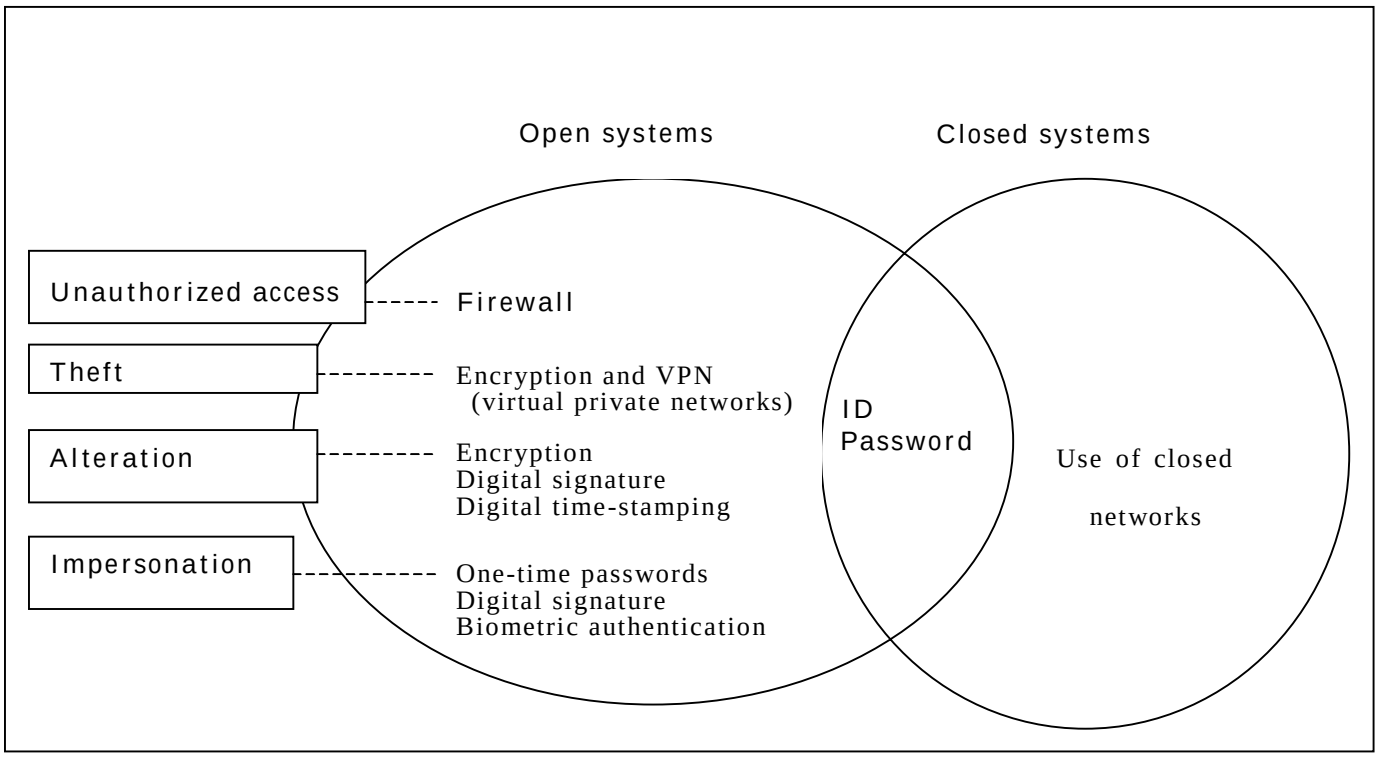
4. Establishing Information Security Measures

(1) Importance of Properly Combining Information Security Measures

Once information security policy is defined, security levels and detailed content of security measures required for each separate system are determined. With a closed system, primary equipment is located in a computer center and hence risk could be isolated in system divisions, particularly in system operating units. However, with application to main operations of open networks, as typified by the Internet, various security technologies (see Diagram 2) are necessary to ensure required information security levels.

Diagram 2

Examples of Information Security Measures in Open Systems



Nevertheless, these security technologies are not always easy for users to implement because of various constraints such as cost of introduction and its limited circulation. Thus, based on an acceptable level of information security risk and taking costs into

account, each financial institution should draft comprehensive measures by appropriately combining technologies according to the importance of information and information systems and other factors.[17]

(2) Timely and Appropriate Incorporation of New Technology

Electronic authentication using public key cryptography[18] is already established and highly evaluated for providing a higher level of security than passwords. However, since electronic authentication is not very user-friendly, it has not caught on as a method of customer authentication in Internet banking and other sectors.[19] Nevertheless, should IC cards containing private keys and digital certificates come to be sold at a low price and become a general settlement measure, we can expect financial institutions to facilitate the use of public key cryptography.

In addition, new authentication technologies are progressing, such as digital time-stamping (a "digital notary" technology, which allows authentication by a third party of "who created and sent what data and when") and biometric authentication (which uses physical attributes such as fingerprints, retina imaging, handwriting, and voice prints).[20] If, in the future, various conditions for introduction are put in place in tandem with advances in technology and the more widespread use of such technology, or if risks

---

[17] For example, as a way to confirm the identity of a customer (to be definitely sure it is the customer) in Internet banking, a password is normally used, but it is not a foolproof information security measure. Therefore, it is necessary to combine a number of different measures, such as setting transaction amount limits on the administrative side, forewarning users not to use predictable passwords such as their birthdays on the operational side, and diversifying the number of digits on the system side.

[18] Electronic authentication uses an digital certificate issued by the authentication institution to confirm the authenticity of the communicant and verify that the electronic transaction data is not altered with in the middle of the process. For details, refer to “PKI and Electronic Authentication in the Financial Industry”(IMES Discussion Paper Series 99-J-30, available only in Japanese) by the Institute for Monetary and Economic Studies, Bank of Japan.

[19] There are many financial institutions that are attempting to minimize the risk of impersonation not by electronic authentication using public keys, but by combining such methods as establishing different passwords for access and for funds transfers, limiting the accounts which funds can be remitted to, and establishing maximum remittance amounts.

[20] For further details on new verification technologies, please refer to the following two documents both by the Institute for Monetary and Economic Studies, Bank of Japan: “Status and Issues of Digital Time-Stamping Technology” (IMES Discussion Paper Series 99-J-36; available only in Japanese) and “Status and Issues of Personal Authentication Technologies through Biometrics” (IMES Discussion Paper Series 99-J-43; available only in Japanese).

should heighten because of transaction amount limits being raised, it will be a good idea to positively pursue ways to apply new information security technology as the needs arise.

The rapid pace of technological advance with respect to the hardware and software that comprise open systems means that security holes are continuously cropping up, and, if these holes are neglected, they will be left open to hacking and other forms of abuse.[21] Hence, any information concerning security holes must be promptly investigated to determine whether a problem exists, and proper measures implemented if necessary. In this regard, it is desirable to (a) properly evaluate to what degree risks might be brought at that time in the environment, (b) input resources deemed necessary without delay, and (c) promptly implement the necessary measures.[22] It is desirable to keep abreast of developments on the technological front on a regular basis.

(3) Importance of the Proper Implementation of Information Security Measures

Merely devising information security measures on an individual basis will not produce effective results. For example, in taking measures to prevent unauthorized access, merely putting in a firewall[23] is not enough; financial institutions have to be constantly aware of the possibility of unauthorized access and remain vigilant for signs of such invasive activities. By gathering information related to patterns of unauthorized access and firewall holes and implementing appropriate countermeasures, the risk of attack can be lowered. It is also important to prepare for attacks by putting in place emergency measures to minimize damage and to have mechanisms ready for speedy notification[24]

---

[21] Some cases have occurred where, in spite of the discovery of a security hole, the security hole was ignored and usage of the system continued, resulting in damage from unauthorized access from the outside.

[22] The person responsible for information security should oversee critical responses necessary to maintain security levels and judge the need for both provisional and drastic responses and the suitability of such responses.

[23] The term "firewall" refers to software and equipment that are located at the point of connection to outside networks and that serve to prevent unauthorized access and outflow of row data by only allowing certain predetermined types of data communication.

[24] There is also a need to suppose events, such as the entire system shutting down or a major impact on

in advance. In addition, the implementation of intrusion tests commissioned to specialized agencies are meaningful to confirm the effectiveness of each security measure. Appropriate implementation and management are necessary to obtain the full benefit of information security measures.

Information security levels can be maintained and improved by establishing a continuous checking cycle of (a) analyzing information security risks (where, to what extent, and what type of risk), (b) devising and implementing both technology- and system-based countermeasures for risks recognized, (c) educating and training employees (including part-timers and subcontractors), (d) confirming the status of implementation through information security audits, and (e) ensuring that audit results are reflected in future risk analysis.

One particular consequence of the greater amount of distributed processing effected by systems is that the weak points of information security measures may be left unnoticed. Additionally, as time passes, traditional security measures become inadequate because of changes in the technological environment. Specifically, there are not a few cases that factors to damage information security in systems using the Internet are always appearing. In response to that, we have to keep on updating countermeasures. In such cases, if a checking mechanism is already established, periodic inspections can be conducted to keep abreast of new risks and plan for effective responses by the entire organization.

5. In Closing

As described above, in order for financial institutions to make the most of IT revolution to develop their businesses, they will need to become sufficiently aware of the

---

services because of an attack on information security; contingency plans should include a response to information security infringement.

importance of information security and take the appropriate countermeasures.

Of course, given that the specifics and level of risk management required will vary greatly depending on the system employed and the business activities of each financial institution, and also given the dramatic changes stemming from technical innovation, there is no single prescription for safety. Each financial institution will have to constantly update its own response while referring to the various guidelines and other relevant information published by international organizations, standardization organizations, and other institutions.

The Bank of Japan is committed to supporting such efforts by financial institutions and will follow the progress made by each financial institution in its management of information security risk from individual financial institution's risk management view. As stated in "Principles for On-site Examination and Off-site Monitoring for Fiscal 2000," the Bank will continuously endeavor to obtain an accurate picture of conditions at financial institutions and foster their implementation of required measures, including through the Bank's targeted examinations with an emphasis on information security.[25]

[25] Some central banks in Europe and the United States publish checklists related to information security and conduct inspections focusing on IT.

(Attachment)

Checklist of Information Security Measures for Systems That Make Use of the Internet

The intended usage of this checklist:

This checklist has been prepared for financial institutions to use as a reference when checking the status of their own information security risk management system. The checklist points out major items for checking information security measures in individual systems that use the Internet.

Things to keep in mind when looking through the checklist:

This checklist emphasizes points relevant to the increasing risks that are incidental to the move toward open systems, as well as new risks that might occur. For this reason, the checklist does not touch on such points as security measures for buildings and facilities at computer centers. In addition, this checklist is not assumed to be applicable to all systems within an organization (for questions concerning points not mentioned here, refer to the appropriate guidelines officially promulgated by pertinent organizations).

April 18, 2000

Bank Examination and Surveillance Department

Bank of Japan

I. Important Points in Formulating Information Security Measures

1. Formulating an Information Security Policy
(1)Are the purpose and targets of information security measures clearly defined? (2)Are the organizational and administrative systems for promoting of information security measures clearly defined? (3)Are the duties and responsibilities of all executives and staff dealing with information security measures clearly defined? (4)Is there an understanding of the information security risks (including obstruction of business, theft and alteration of information, and impersonation) facing the entire organization and have measures for dealing with those risks been examined and implemented? (5)Have policy measures in cases where the provision of service is interrupted through obstruction or unauthorized action been clearly defined? (6)Have procedures to handle exceptional cases where information security policies cannot be properly applied been clearly defined? (7)Have rules on proper use of information security policies been clearly defined when using outsourcing or vendors?

II. Important Points in Deciding Information Security Measures

1. Deciding Information Security Measures
(1)Have information security measures been decided on the basis of an information security policy? (a) Have the importance of certain information, the extent of the risk, and similar factors been taken into consideration so that a comprehensive plan that includes both business and system-related features can be devised? (b) Is there a process built into the information security policy whereby the development of measures that do not follow the policy can be approved? (c) Has a system been set up whereby the circumstances surrounding the use of outsourcing or vendors can be confirmed? (2)Are information security measures reviewed periodically based on the latest information on security, taking into account the importance of information and level of risks? (3)Are weaknesses in technology and management of systems that arise from connection with the Internet or the probability of the occurrence of information security risks understood based on the latest information on security? (4)When the network is connected to vendors or similar entities, are the information security measures of those entities checked?

III. Important Points in Terms of Management-Related Considerations with Respect to Information Security Measures

1. Involvement of Management
(1)Have information security policies been approved by management? (2)Is management aware of the extent and location of information security risks? (3)When improprieties that hinder the operation of systems are detected, are they directly reported to management, and can management promptly issue instructions to take control of the situation? (4)Have contingency plans that include measures to address information security infringements been approved by management?
2. Involvement of Information Security Coordination Division
(1)Does an information security coordination division (or the person responsible for coordinating information security) go through the items of the information security measures that have been devised based on the results of the evaluation of information security? (2)Does such division periodically call for the review of information security measures by

each function? (3)It is desirable that the division is independent from the system business unit.
3. Involvement of Audit Division
(1)Does an audit division, acting independently of any departments that are under internal audit, carry out audit to verify such aspects as an institution's adherence to information security policy and the adequacy of information security measures? (2)It is desirable that external audits are used when the importance of a system so warrants.
4. Involvement of Legal Division
(1)Does the legal division check the extent of responsibilities of its institution as defined in the transaction agreements when initiating new business via the Internet? (2)Does the division check legal risks that cannot be covered by transaction agreement due to changes in legislation?

IV. Important Points Regarding New Information Security Measures

1. Firewalls
(1)Have appropriate measures been devised regarding the introduction and implementation of firewalls? (a) Have appropriate rules for communication been formulated and appropriately implemented? (b) Is there appropriate control of access, including physical access, to the firewall apparatus? (c) Has a system for the precise monitoring of communication data that passes through the firewall been formulated and appropriately implemented? (d) Is a record of communication through the firewall kept as a log? (e) Have documents on the design of firewalls been properly filed? (2)Has information on security holes in firewalls been gathered, and the necessary countermeasures taken? (3)It is desirable that the reliability of firewalls is periodically confirmed through such measures as intrusion tests conducted by specialists.
2. Encryption
(1)Is highly confidential information encoded when it is transmitted or received? (2)Have appropriate rules of application been formulated and properly implemented for the use and control of codes? (Are the rules controlling encryption keys defined clearly?) (3)It is desirable that suitable security evaluations are conducted when using encryption. (4)In using public keys, are private keys appropriately dealt with as pair keys? (a) Are there periodic confirmations based on the latest security information to verify that security problems, such as compromising the private key used in key generation, are not occurring? (b) When delivering or storing keys, has consideration been given to protecting the confidentiality and validity of keys by using tamper resistance device (such as features to erase a key that someone has tried to steal)?
3. Digital Signatures
(1)Is user verification through digital certificates or similar confirmation procedures effected when risks are exceedingly large, such as the transfer of large amounts of money? (2)It is desirable that a digital signature is used in order to prevent leaks and alterations when sending or receiving important information. (3)When a financial institution operates its own CA (Certification Authority), are there rules regarding its usage, and is such usage in accordance with such rules? (4)When certification is entrusted to a third-party facility, is the degree of reliability, capability, and range of responsibility of the said CA thoroughly considered?
4. Business Obstruction Countermeasures

(1)Are there alternative measures to ensure continuance of business operation, on the assumption that there could be repetitive access attacks that exceed the capacity of a system in a short period and aimed at causing servers to go down (Denial of Service attack)?
(2)Have systems for detecting viruses or operational rules related to anti-virus measures been formulated and appropriately implemented for the entire organization?

V. Important Points Regarding Existing Information Security Measures

1. Managing User IDs and Passwords
(1)Are measures in place to prevent the unauthorized use of user IDs? (a) Is log-in prevented following a certain number of failed attempt? (b) It is desirable that a one-time password (a password that is generated through special equipment and changed every time it is used) should be employed, if necessary, for all system IDs (including privileged access IDs). (2)Are appropriate password controls being implemented? (a) Are passwords set and changed by the individual users themselves? (b) Has consideration been given to prevent the theft of passwords? (c) It is desirable that users regularly change passwords.
2. Countermeasures against Obstruction, and Data Maintenance
(1)In ensuring back-up copies of data and taking communication records, have the timing and method of acquisition, saving formats, and data saving period been set and adequately implemented? (2)Has necessary information been acquired for inspection records (user IDs, functions/data used, existence of alterations to such data, day and time of use, machine/network used, etc.)?
3. Others
(1)Are there appropriate and required evaluations of performance, including the response to data volume, which also take account of peak-time volume? (2)As for resource management, it is desirable that regular checks are in place to ensure that no programs are inappropriately installed, and that systems are not improperly used.

VI. Important Points Regarding Risk Management of System Operations

1. Monitoring System Operations
(1)Have appropriate monitoring systems been formulated for monitoring practices including the improper use of user IDs? (a) Have appropriate countermeasures been prepared to respond to signs of unauthorized access, including emergency measures? (b) In the operation of systems, it is desirable that consideration is given to ensure that the system is not overly dependent on vendors or specific individuals. (2)Are there procedures in place for dealing with possible information security problems, and have they been disseminated throughout the organization?
2. Managing System Changes
(1)Have rules been formulated for system changes? (a) Is access to software and hardware by unauthorized individuals restricted? (b) When hardware is disposed of, is all data erased without divulging important information? (c) With respect to the installation of hardware and software by vendors, is it confirmed that such installation is correctly effected and no unauthorized acts are effected?
3.Formulating Contingency Plans
(1)Have effective measures against the obstruction at safeguards been formulated?

(a) Are there manuals that set out procedures to respond to emergencies? (b) In revising systems, have appropriate procedures been formulated? (c) Are manuals revised to reflect system modifications, and is the list of emergency contact staff updated? (2)It is desirable that drills be conducted periodically with respect to contingency plans and appropriate modifications made based on the results of such drills.
4. Outsourcing and Vendor Management
(1)If the institution outsources system management, does it confirm mechanisms for information security management at the outsourcing firm, and has it monitored other conditions? (2)When a vendor is commissioned with a task, are the conditions clearly defined from the standpoint of information security, and is appropriate monitoring effected to ensure such conditions are being followed?
5. Training System Personnel
(1)Are personnel given necessary knowledge and technical expertise regarding information security? (2)Are employees (including part-timers) given enough opportunities to learn about information security? (3)It is desirable that there is a system in place whereby employees are informed of the latest information security matters.